UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/838,239	04/20/2001	Srikanth Natarajan	10007591/020	9191

7590 12/22/2009

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
SHAW, PELING ANDY	
ART UNIT	PAPER NUMBER
2444	

MAIL DATE	DELIVERY MODE
12/22/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte SRIKANTH NATARAJAN
and DARREN D. SMITH

Appeal 2009-001387
Application 09/838,239[1]
Technology Center 2400

Decided: December 22, 2009

Before LEE E. BARRETT, JEAN R. HOMERE, and STEPHEN C. SIU, *Administrative Patent Judges*.

BARRETT, *Administrative Patent Judge*.

DECISION ON APPEAL

This is a decision on appeal under 35 U.S.C. § 134(a) from the final rejection of claims 1-8. We have jurisdiction pursuant to 35 U.S.C. § 6(b).

We reverse.

---

[1] Filed April 20, 2001, titled "Method and System for Consolidating Network Topology in Duplicate IP Networks." The real party in interest is Hewlett-Packard Development Company L.P.

STATEMENT OF THE CASE

The invention

The invention relates to a method and system for managing a computer network. A collection station (e.g., CS in Fig. 1) is assigned a management domain identifier uniquely associated with a management domain in which each collection computer resides and a trust name flag. This information is received in at least one management station (e.g., MS 105 in Fig. 1). The trust name flag can be used by the management station to determine whether or not the hostname is name trustworthy, i.e., whether or not to use or trust the hostname being reported by the collection station. Spec. ¶¶ [0030]-[0031].

The claims

Claim 1 is reproduced below:

> 1. A method of managing a computer network, comprising the steps of:
>
> assigning to at least one collection computer a management domain identifier uniquely associated with a management domain in which each collection computer resides;
>
> receiving, in at least one management computer, information from the at least one collection computer that includes the management domain identifier and a trust flag to indicate a binary setting;
>
> deciding whether the at least one management computer should resolve a hostname being reported by the at least one collection computer based on the binary setting of the trust flag; and

maintaining within the at least one management computer a database of the information accessed using the management domain identifier.

The references

Nelson	US 5,577,252	Nov. 19, 1996
Pulsipher	US 5,948,055	Sep. 7, 1999
Lecheler	WO 00/49769	Aug. 24, 2000

The rejections

Claims 1-4, 7, and 8 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Lecheler and Nelson.

Claims 1-8 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Pulsipher and Nelson.

CONTENTIONS

The Examiner finds that Lecheler and Pulsipher describe the limitations of the rejected claims except for the limitations of "a trust flag to indicate a binary setting" and "deciding whether the at least one management computer should resolve a hostname being reported by the at least one collection computer based on the binary setting of the trust flag." The Examiner finds:

> Nelson shows (claim 1) a trust flag to indicate a binary setting and deciding whether the at least one management computer should resolve a hostname being reported by the at least one collection computer based on the binary setting of the trust flag (column 1 line 54-column 2 line 2; column 6 line 62-column 7 line 18; column 9

> lines 1-23; column 11 line 65- column 12, line 2: name resolution based upon trust) in an analogous art for the purpose of implementing secure name servers in an object-oriented system.

Final Rej. 3 and 5-6. The Examiner concludes that it would have been obvious to modify Lecheler and Pulsipher with Nelson's functions of name resolution based on trust. Final Rej. 3, 6. In particular, the Examiner finds that name resolution involves an assurance of security where "contexts" in different name servers have the same encapsulated principal. Ans. 9. The Examiner states that those of ordinary skill in the art knew that bits were used to set flags. Ans. 9-10.

Appellants argue that Nelson does not relate to resolving a hostname should a trust status indicate the need for a resolution, i.e., it does not teach "deciding whether the at least one management computer should resolve a hostname being reported by the at least one collection computer based on the binary setting of the trust flag." Br. 5. It is argued that Nelson discloses that a way of allowing a name server to continue across a name server boundary is to have "the original context and the context in the second name server have the same encapsulated principal" (col. 7, ll. 12-15) and that if the two contexts do not encapsulate the same principal, then "name server A cannot continue with the name resolution" (col. 11, ll. 62-64). Br. 5. It is argued that the "encapsulated principal" relied upon by the Examiner "would not have taught or suggested Appellants' information from a collection computer that includes a management domain identifier and a trust flag to indicate a binary setting." Reply Br. 2. Appellants also argue that "the 'encapsulated

principal,' as the Examiner relies on, does not appear to be used as a trust flag for the purpose of deciding whether a management computer should resolve a hostname, but rather, the 'encapsulated principal' as referred to in the Nelson et al. patent seems to be for a name server 'B' to return a copy of object 'X' that is found to have the same 'encapsulated principal.'" *Id.*

Appellants also argue that Nelson is silent as to "a trust flag to indicate a binary setting." Br. 5.

ISSUE

Have Appellants shown that the Examiner erred in concluding that it would have been obvious to modify Lecheler and Pulsipher to provide "a trust flag to indicate a binary setting" and "deciding whether the at least one management computer should resolve a hostname being reported by the at least one collection computer based on the binary setting of the trust flag," as recited in claim 1 and similar limitations in claim 8 given the teachings of Nelson?

PRINCIPLES OF LAW

Obviousness requires that the differences between the subject sought to be patented and the prior art are such that the subject matter as a whole would have been obvious to one of ordinary skill in the art and that the combination teaches all claim limitations. 35 U.S.C. § 103(a).

FACTS

Specification

The Specification describes adding two additional fields to the topology node object representing the collection computer: a management domain identifier and a trust name flag. The management domain identifier can be an attribute of the collection station object and the trust name can be a single bit flag in the collection station object. ¶ [0030].

The Specification describes the trust name flag as follows:

> The trust name flag can be used by the management station to determine whether or not the hostname is name trustworthy, i.e., whether or not to use or trust the hostname being reported by the collection station. Thus, if the trust name flag is set to, for example, one, then the hostname of the network element as reported from the collection station will be used as the name of the network element, otherwise it will be recomputed at the management station based on, for example, the IP address of the interfaces associated with the network element or node.

¶ [0030].

Nelson

Nelson describes a secure naming model for objects in an object-oriented system, wherein names are bound to objects within context objects. *See* Abstract.

An object in an object-oriented system typically comprises a collection of data (state data) and a set of functions (operations) for manipulating the collection of data. Each object corresponds to an object

manager. The object manager is a server that performs the operations for the object and that maintains the state data in the object. Col. 1, ll. 14-21.

Typically, a client sends a message to the object to perform an operation. The operation usually returns a return value to the client after completion of the operation. Col. 1, ll. 22-31.

A naming service is usually employed to simplify access to objects in an object-oriented system. A naming service associates names to the objects within the system. The functions of a naming service are typically performed by one or more name servers. Each name server contains a list of name to object associations. Col. 1, ll. 32-37.

A client typically issues requests to a name server to resolve a requested name and return a duplicate of the object corresponding to the requested name. In a typical object-oriented system, each name server can create duplicates of the objects. As a consequence, the access to the name servers should be secure. Col. 1, ll. 38-43.

Nelson relates to providing a secure naming model for the objects in the object-oriented system, wherein names are bound to objects within context objects. The context objects are implemented by name servers. A client requiring a named object requests that a context object "resolve" the name for the object. The name server that implements the context returns a duplicate of the desired object. If a name resolution involves more than one name server, an assurance of security is provided by the first name server to the second name server. For example, if a name resolution were to cross between name server A and name server B, name server B would require

name server A to provide assurance that system security is not being breached. The assurance is provided according to several methods. First, each of the name servers involved in the name resolution "trusts" the other named servers involved in the name resolution. Such a "trust" method requires no additional authentication. Alternatively, the assurance is provided by implementing context objects in name servers, such that the context objects encapsulate the same principal. In this case, the name resolution is allowed to continue since the context in the second name server has the same access rights as the context in the original name server. Alternatively, the assurance is provided by aborting the name resolution and requiring the requesting client to authenticate itself. Col. 1, l. 51 to col. 2, l. 2; Col. 7, ll. 5-40.

ANALYSIS

The issue depends on the teachings of Nelson.

Nelson describes name resolution in an object-oriented system in which a name server returns a duplicate of the object corresponding to the requested name. Nelson is not related to managing a computer network, does not have a collection computer or a management computer, and does not involve resolving hostnames. The Examiner finds that Nelson is in an analogous art. Final Rej. 3. Since at least Pulsipher deals with objects, we assume that Nelson is analogous art. Nevertheless, the big difference in environments makes it difficult to apply Nelson.

Initially, the Examiner does not identify what corresponds to the claimed "trust flag to indicate a binary setting" in Nelson. The Examiner states that "Nelson shows (claim 1) a trust flag to indicate a binary setting," Final Rej. 3 and 5, but does not point to any specific language. We find that claim 1 of Nelson does not recite any limitation that could be considered a trust flag or a trust flag indicating a binary setting. The Examiner refers to a "trust" flag in Wesley, US Patent 6,076,114 A, column 9, lines 27-41 in an earlier Office Action. Ans. 10. However, Wesley is not part of the stated rejection. Wesley is not considered because the statement of the rejection must expressly contain a mention of all references applied in the rejection. *See In re Hoch*, 428 F.2d 1341, 1342 n.3 (CCPA 1970); *Ex parte Movva*, 31 USPQ2d 1027, 1028 n.1 (BPAI 1993). The Examiner has not stated what quantity in Nelson would be represented by a binary trust flag or why Nelson would have suggested that such information would be sent from a collection computer to a management computer, as claimed.

The next question is whether Nelson suggests modifying Pulsipher or Lecheler to provide the function of "deciding whether the at least one management computer should resolve a hostname being reported by the at least one collection computer based on the binary setting of the trust flag." It is true that Nelson contains the words "trust" and "name resolution" for "resolving" the name of an object. Col. 7, ll. 5-18. However, isolated words do not meet the specific claim limitations. Nelson describes a special connection where two servers "trust" each other and no authentication is required when performing a name resolution. Col. 7, ll. 5-11. However,

Appellants correctly point out that in this case no authentication is required (Reply Br. 1-2), so there is no teaching of resolving a hostname based on a binary setting. The Examiner apparently does not rely on this method of assuring system security, but relies on the method where the contexts on two different name servers have the same encapsulated principal. Ans. 9-10.

The Examiner finds that name resolution based upon trust is taught in Nelson at column 1, line 54 to column 2 line 2; column 6, line 62 to column 7, line 18; column 9, lines 1-23; and column 11, line 65 to column 12, line 2. Final Rej. 4, 6. These portions of Nelson describe three methods of assuring security when name resolution crosses over name server boundaries: first, there is a special connection so that each of the name servers involved in the name resolution "trusts" the other named servers involved in the name resolution; second, the context objects encapsulate the same principal; and third, aborting the name resolution and requiring the requesting client to authenticate itself. Only the first method involves a "trust" relationship. The second method of encapsulating the principal does not involve a trust relationship (col. 9, ll. 5-10). Thus, the Examiner errs in relying on the second method of encapsulating the principal as a method of resolving names based on a trust relationship.

It is also unclear how Nelson's method of name resolution based on encapsulating the principal would have suggested the specific claim limitations. Claim 1 recites that a management computer receives information from a collection computer that includes "a trust flag to indicate a binary setting." In Nelson, "if a name resolution were to cross between

name server A and name server B, name server B would require name server A to provide assurance that system security is not being breached." Col. 6, l. 66 to col. 7, l. 2. Thus, assurances travel outward, not back towards the client (what would be the claimed management computer).

We also agree with Appellants that Nelson does not relate to resolving a hostname should a trust status indicate the need for a resolution, i.e., it does not teach "deciding whether the at least one management computer should resolve a hostname being reported by the at least one collection computer based on the binary setting of the trust flag." Nelson relates to resolving a name of an object so that a name server can return a duplicate of the object corresponding to the requested name. Nelson does not describe resolving a "hostname" and the Examiner has not explained why Nelson's teaching would suggest such a modification. Nelson does not indicate a binary trust flag sent from a collection computer to a management computer. Therefore, Nelson does not suggest "deciding" whether to resolve a hostname based on the setting of the trust flag. One of ordinary skill in the art would not find Nelson to teach or suggest the claim limitations.

CONCLUSION

Appellants have shown that the Examiner erred in concluding that it would have been obvious to modify Lecheler and Pulsipher to provide "a trust flag to indicate a binary setting" and "deciding whether the at least one management computer should resolve a hostname being reported by the at least one collection computer based on the binary setting of the trust flag," as

recited in claim 1 and similar limitations in claim 8 given the teachings of Nelson. Accordingly, the rejection of claims 1-4, 7, and 8 under 35 U.S.C. § 103(a) over Lecheler and Nelson is reversed. The rejection of claims 1-8 under 35 U.S.C. § 103(a) over Pulsipher and Nelson is reversed.

REVERSED

rwk

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400